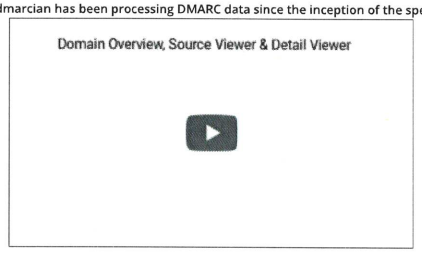
DMARC SaaS Platform

dmarcian's DMARC SaaS platform receives, processes and classifies mail observed from your domain namespace and makes sense of it for you. The native XML format in which DMARC data is transmitted is not intended for human consumption. Our platform visualizes the data in powerful and meaningful ways so you can quickly identify authentication gaps (SPF/DKIM) and unauthorized use of your domains.

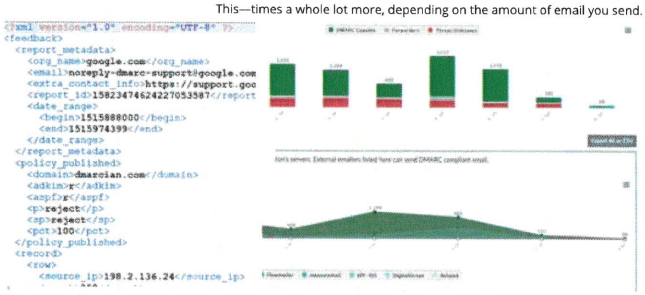
In addition to aggregating DMARC data, our platform provides domain administration teams with the necessary features to adopt DMARC with clarity and confidence. The dmarcian reporting platform sits atop the most accurate source classification engine in the industry and affords users with assurances of the true origin of a particular mail stream.

dmarcian has been processing DMARC data since the inception of the specification in 2012.



Without dmarcian

This—times a whole lot more, depending on the amount of email you send.



With dmarcian

DMARC's XML feedback contains useful information, and **dmarcian** helps you make sense of it.

Getting started with DMARC

DMARC, (Domain-based Message Authentication Reporting, & Conformance) an open source standard, uses a concept called *alignment* to tie the result of two other open source standards, SPF (a published list of servers that are authorized to send email on behalf of a domain) and DKIM (a tamper-evident domain seal associated with a piece of email), to the content of an email. If not already deployed, putting a DMARC record into place for your domain will give you feedback that will allow you to troubleshoot your SPF and DKIM configurations if needed.

Adopting DMARC involves creating a DMARC record, publishing it, and using the information that is generated to gain insight and control over the way your domains are handling email. DMARC helps legitimize your email by doing two things:

- Gives feedback about the email itself, including information about SPF and/or DKIM alignment.
- Tells email receivers (like Gmail and Yahoo) how to handle messages that fail to align with those protocols.

dmarcian can assist your organization in every step of the way, from deploying the underlying technologies of DMARC, to making sense of the data that it generates, to gaining full insight and control to the way your email domains are being used.

Assess

The work required to deploy DMARC is directly related to the size and complexity of an organization's email infrastructure. DMARC is a domain-based email control and email domains are a shared resource within most organizations, with use spanning from employees to entire departments, external parties that send email on behalf of the organization, and the organization's own internet-facing applications.

When deploying DMARC, it's best to roll it out across all of an organization's domains instead of focusing on individual domains. When DMARC is deployed at an organization across the entire domain portfolio, the process of deployment itself becomes much easier as there is complete organizational visibility, and managers get new tools to ensure *all* email is being sent in compliance with the organization's standards.

Publishing a DMARC record

To start generating DMARC data, you must first publish a DMARC record for each domain you wish to monitor. **dmarcian's** DMARC Record Wizard makes it easy to create a DMARC record.

A DMARC record exists as part of your Domain Name System (DNS) record, which routes traffic on the internet. You can include additional information in the DNS, like your domain's DMARC record—a text entry within the DNS record that tells the world your email domain's policy based on the configured SPF and DKIM protocol.

Here are instructions on how to publish a DMARC record with your DNS host.

Once you've published DMARC records, DMARC data will typically begin to generate within a day or two in the form of reports that give you insight into the way your domains are handling email. These reports are XML-based and can be difficult for humans to read and make sense of, especially when they can number in the thousands. **dmarcian's** DMARC SaaS Platform specializes in processing these reports and identifying the steps needed so that DMARC can be more easily deployed throughout an organization. We categorize sources of email and present you with DMARC compliance status (based on email source, DKIM and SPF), and we alert you if there are any potential threats to or abuse on your domains.

Getting data to dmarcian

There are different ways of getting data processed by **dmarcian**:

- **Send Data Directly to dmarcian.**
  The most convenient option to have data processed is by sending your DMARC reports directly to **dmarcian** for processing. Upon creation of your account, you will receive an email address where you can send DMARC reports to be processed.
- **Forward Data to your dmarcian account**
  If you already have DMARC reports being generated, or don't wish to send reports directly to **dmarcian**, you can forward DMARC reports to the address provided when you register.
- **Upload Data Directly to dmarcian.**
  If you already have DMARC XML data, you can upload it using the XML-to-Human Converter. You will be given a detailed report of your data, but your data history will not be stored unless you are logged in.

DMARC policy

For an email message to be considered DMARC-compliant, the domain found in the "From:" header must match the domain validated by SPF or the source domain found in a valid DKIM signature. If the domains match and at least one

DKIM Only	✓	@client.net	client.net	@sample.net
SPF Only	✓	@client.net	sample.net	@client.net
FAIL	✗	@client.net	sample.net	@sample.net

** If SPF or DKIM is absent, this individual check will fail, leaving only the other to result in a pass. If SPF and DKIM are absent, automatic DMARC fail.*

A DMARC policy allows a domain owner to indicate that their messages are protected by SPF and/or DKIM and tells the recipient what to do if none of these are verified on a particular piece of email, such as marking it as junk mail or rejecting delivery of the message. Domain owners can set their DMARC policy (referred to as "*p=*") to determine what is done to non-compliant email:

- **Monitoring** (p=none) no impact on mail flows (*only DMARC feedback is collected*)
- **Quarantine** (p=quarantine) messages that fail DMARC (*e.g. move to the spam folder*)
- **Reject** (p=reject) messages that fail DMARC (*don't accept the mail at all*)

The Road to p=reject

DMARC policies typically start at a state of p=none, which is a monitoring phase that gives visibility into how your domain is being used and how SPF and/or DKIM are functioning, and moves towards a policy of p=reject. Reject instructs email receivers to refuse to accept email that fails DMARC. By default, email that fails under a reject policy is not accepted. This behavior is a great control against the sending of unauthorized email making use of your domain.

It is estimated that only 30% of organizations who start the process of deploying DMARC ever complete the process. The challenge isn't the specification itself but with the email ecosystem and the interpretation of the feedback that is provided. The process of adopting DMARC into an organization can be daunting, but with the proper partner, it can be easily managed.

Troubleshooting

DMARC Record Issues

Issues in a DMARC record may prevent DMARC data from being reliably generated. Use the DMARC Inspector to inspect your domain and discover any issues with your DMARC record.

Common record issues include:

- The v=DMARC1 tag is not optional and is case sensitive. Remember: DMARC1 must be in caps!
- Addresses inside rua and ruf tags must be in URI format (i.e. mailto:user@example.com)
- Your DMARC record must be located at _dmarc.[yourdomain].com

Trouble Delivering DMARC Data to dmarcian

For active sending domains, you will typically begin to see DMARC data within a day or two. If your domain does not send a significant amount of email, it may take longer for DMARC data to appear. If you are having trouble generating data in your **dmarcian** account, try the following resources:

- Have not received any XML reports
- External Destination Verification - What is this?

If you are still having trouble getting DMARC data into your account, contact us and let us know about your issue.

DMARC SaaS Platform

To turn thousands of XML records into something useful, **dmarcian** processes DMARC data using a complex set of identifiers. We categorize sources of email and present you with DMARC compliance status (based on email source, DKIM and SPF), and we alert you if there are any potential threats or abuse on your domains.

Deployment Services

The challenge with deploying DMARC isn't the specification itself, but with the email ecosystem and the interpretation of the feedback that is provided. **dmarcian** offers a project-based approach for policy enforcement tailored to your organization's needs.

Dedicated Support

Although deploying DMARC can be viewed as a one-time technology upgrade, managing and maintaining DMARC compliance needs long-term effort to remain effective. **dmarcian** can help with managing DMARC-related incidents, regular data reviews, monitoring ongoing compliance, and embedding DMARC into daily operations.